Richard Akerman
Présentation au Comité spécial sur la réforme électorale
Évaluation du vote électronique et en ligne dans le cadre des élections nationales au Canada

Section 1 : Sommaire

Sommaire

Le recours à des dispositifs de vote en ligne et de vote électronique viendrait grandement accroître les risques, sans offrir suffisamment d'avantages pour compenser ces risques.

Considérations :

- L'utilisation du vote en ligne à grande échelle permettrait une vaste coercition des électeurs, notamment l'achat de votes.
- Les innombrables composants logiciels et matériels qui seraient nécessaires pour marquer, transmettre, recevoir et compter les bulletins de vote électronique représentent un risque élevé irraisonnable pour la chaîne de possession du bulletin de vote.
- Les ministères du gouvernement canadien ont déjà été victimes de cyberattaques de la part d'États-nations.
- Les experts en sécurité informatique nous avertissent que le vote en ligne n'est pas sécuritaire.
- Les experts en sécurité nationale nous avertissent que le vote en ligne n'est pas sécuritaire.
- Les données probantes issues des sciences sociales indiquent que le vote en ligne n'augmentera pas la participation des électeurs.

Pour ces raisons, le Comité spécial sur la réforme électorale devrait recommander de ne pas utiliser le vote en ligne et le vote électronique dans le cadre des élections canadiennes.

Évaluation selon les principes

1. **Efficacité et légitimité** : sans bulletins de vote papier à compter, les accusations de piratage du système de vote peuvent mener à la remise en question de la légitimité de l'élection.
2. **Participation** : le vote en ligne ne permet pas une hausse significative de la participation électorale et est surtout utilisé par les électeurs qui auraient voté dans un bureau de vote de toute façon.
3. **Accessibilité et inclusion** : le vote en ligne s'accompagne d'une complexité technologique visible et cachée et exclura les personnes sans un bon accès Internet.
4. **Intégrité** : les risques pour la sécurité que posent le vote en ligne et le vote électronique sont si importants que le Parlement australien a classé les risques pour l'intégrité du système dans la catégorie des risques catastrophiques.
5. **Représentation locale** : le vote en ligne et le vote électronique n'ont aucune incidence sur la représentation locale.

Section 2 : Considérations et recommandations

Considérations relatives au vote à distance

Le processus de marquer un bulletin de vote seul et sans témoin derrière un isoloir dans un bureau de vote n'est pas apparu comme par enchantement; il a été spécialement choisi et conçu pour réduire le risque de coercition.

Par **coercition**, on entend le fait d'influencer une personne à voter pour un parti ou un représentant en particulier, par une récompense (p. ex. approbation sociale, achat de votes) ou par des menaces (p. ex. menaces de violence ou menaces de congédiement de la part de l'employeur). Le risque de coercition existe depuis que le vote existe.

Lorsqu'une personne autre que l'électeur peut voir le X sur un bulletin de vote ou que l'électeur peut prouver à un tiers comment il a voté après que le bulletin a été enregistré, le risque de coercition devient très élevé.

C'est donc dire que presque tout système de vote à distance, y compris le vite en ligne, s'accompagne d'un risque de coercition accru.

De plus, le vote à distance entraîne des risques pour la **chaîne de possession**. La chaîne de possession est une exigence liée à l'intégrité de l'élection; les bulletins de vote et les séries de bulletins de vote sont toujours gardés en lieu sûr et sous surveillance. Les observateurs doivent être choisis parmi les factions politiques opposées afin d'empêcher toute collusion pour modifier les bulletins de vote.

Une solide chaîne de possession permet de veiller à ce que les bulletins de vote, une fois marqués, soient protégés contre toute altération ou perte, et toute la série de bulletins de vote (p. ex. contenus dans une boîte de scrutin) est protégée de la même façon, ainsi que contre l'ajout de bulletins de vote qui n'ont pas été remplis par des électeurs (« bourrage des urnes »).

Le vote en ligne peut sembler avoir une très courte chaîne de possession, de l'ordinateur au serveur de vote, en passant par Internet, mais il s'agit d'une mauvaise compréhension des véritables étapes qui doivent être suivies pour exprimer un vote par Internet. En réalité, les « mains » dans lesquelles passe un bulletin de vote électronique pour être compté sont presque innombrables. Le logiciel de vote, le navigateur Web, le système d'exploitation, les autres applications de l'ordinateur, les périphériques réseau et les couches logicielles du serveur de vote central pourraient tous interférer avec l'acheminement du bulletin de vote, en le modifiant ou en le détruisant, ou encore en ajoutant d'autres bulletins de vote. Très concrètement, la chaîne de possession d'un bulletin de vote en ligne est constituée de tous les gens qui ont écrit l'une des millions de lignes de logiciel des systèmes d'exploitation, des applications et des périphériques réseau qui traiteront le bulletin de vote numérique. Voilà qui est tout un témoignage de confiance envers une foule d'étrangers. Pour cette raison, le risque du vote en ligne pour la chaîne de possession est extrêmement élevé.

Considérations relatives au vote technologique

À première vue, l'introduction de la technologie informatique dans le processus de vote peut sembler lui ajouter un côté très pratique et efficace. Cependant, un examen plus poussé des caractéristiques particulières d'un processus de vote révèle que la technologie informatique ne satisfait pas à toutes les exigences nécessaires en matière de vérifiabilité et de sécurité; un papier et un crayon sont, en réalité, les techniques qui conviennent le mieux.

La **vérifiabilité**, soit la capacité de faire la preuve que les votes ont été correctement comptés, est essentielle pour la confiance du public envers les élections. En cas d'élections hautement litigieuses, il est crucial de pouvoir démontrer à toutes les factions politiques que les votes ont été comptés comme il se doit. Le comptage des bulletins de vote papier en public, sous la supervision d'observateurs de chacun des partis politiques, est une excellente méthode, facile à comprendre, qui offre un résultat clair et transparent. En présence d'un résultat serré, les bulletins de vote peuvent être soumis à un dépouillement judiciaire pour qu'une décision définitive soit prise.

Comparons maintenant le comptage public des bulletins de vote papier au comptage des votes faits en ligne ou par un système de vote électronique « sans imprimé », dont le résultat sort tout simplement de la boîte noire de l'ordinateur. Il n'y a aucune autre preuve qu'un nombre à l'écran. Il n'existe aucune possibilité significative de recomptage; il n'y a rien à recompter. Ce n'est pas parce que l'ordinateur est une machine de comptage parfaite, c'est parce qu'il n'y a tout simplement pas de preuves concrètes qui peuvent être examinées autres que ce qui se trouve déjà dans l'ordinateur. Et ce qui se trouve dans l'ordinateur a pu être manipulé de nombreuses façons par des cyberattaqueurs.

Voilà qui nous mène à la question de la **sécurité**. Le monde virtuel est rempli de menaces, et des menaces différentes de celles du monde physique. Dans le cadre des élections faites sur papier dans un endroit physique et dont les votes sont comptés manuellement qui ont cours au Canada, les bulletins de vote sont comptés dans plus de 60 000 bureaux de vote. Pour interférer avec l'enregistrement ou le comptage des bulletins aux bureaux de vote à grande échelle, il faudrait qu'une foule de personnes soit physiquement présente dans les bureaux de vote et prenne beaucoup de risque pour agir ainsi dans un endroit où il y a de nombreux observateurs des factions politiques opposées.

Contrairement au monde physique, le monde virtuel offre trois nouvelles capacités aux cyberattaqueurs :

1. Distance
2. Automatisation
3. Échelle

Un cyberattaqueur qui tente de perturber une élection en ligne n'a même pas à se trouver dans le même pays. Il peut attaquer à **distance**, et même lorsque les attaques ont été attribuées à des États-nations, nous constatons bien souvent que les conséquences de la perpétration d'une telle attaque ont été minimes.

De plus, un cyberattaqueur peut tirer profit de la puissance d'un ordinateur pour **automatiser** des tâches. En fait, des balayages automatiques pour déceler les vulnérabilités des ordinateurs se déroulent constamment sur Internet, à la recherche de systèmes à compromettre. Le logiciel de balayage utilisé peut incorporer certaines des

connaissances spécialisées les plus sophistiquées au monde en matière d'attaque informatique, et ce, à la simple pression d'une touche. C'est donc dire qu'un seul cyberattaqueur peut effectuer des attaques très sophistiquées.

Il importe de ne pas croire qu'un seul individu assis devant son ordinateur cherche à attaquer un seul autre ordinateur. L'automatisation et les ressources informatiques bon marché très répandues font en sorte que les attaques peuvent se dérouler à **grande échelle**. Ainsi, un seul ordinateur peut en attaquer de nombreux autres simultanément, mais en pratique, ce sont de nombreux ordinateurs (parfois des milliers d'ordinateurs d'un « réseau zombie ») qui ciblent un seul ordinateur, un petit groupe d'ordinateurs ou des milliers d'ordinateurs. L'objet de l'attaque peut être l'intrusion, mais simplement aussi un « déni de service », c'est-à-dire que le système informatique ciblé reçoit tellement de demandes qu'il ne peut plus fonctionner correctement.

Puisqu'une élection ne peut être tenue de nouveau, même un déni de service (qui est une attaque très simple à faire) pourrait s'avérer catastrophique le jour de l'élection. Des attaques plus sophistiquées, y compris celles qui compromettent les systèmes de vote et altèrent les votes, pourraient être encore plus dévastatrices, surtout si l'attaque n'est découverte que des mois après l'élection.

Recommandations

- Il faut prendre le temps qui faut; il n'est pas nécessaire de précipiter la démarche d'analyse pour prendre une décision concernant le vote en ligne et le vote électronique.

- Le vote en ligne est un sujet de recherche en sciences informatiques, et non un sujet d'essai. Puisque le directeur général des élections Mayrand a demandé au Comité de lui donner des orientations de recherche, il faut réunir un comité d'experts en informatique pour définir un programme de recherche. Cette recherche pourrait permettre de relever les défis en ce qui concerne les principes de la légitimité, de l'accessibilité et de l'inclusion, ainsi que celui de l'intégrité soulevée plus tôt.

- Le comité d'experts en informatique pourrait envisager d'orienter la recherche pour répondre aux questions suivantes :
    - Comment réduire le risque de coercition lors de l'utilisation du vote à distance?
    - Comment améliorer la chaîne de possession lors de l'utilisation du vote en ligne? Comment permettre un vote vérifiable de bout en bout?
    - Comment mettre en place des mesures de sécurité adéquates pour le vote en ligne dans un monde où les citoyens disposent d'appareils non sécurisés et où certains États-nations sont des cyberattaqueurs sophistiqués?

- Les machines de vote électronique (y compris la technologie de comptage) doivent être considérées comme des *ordinateurs* de vote électronique; elles présentent des risques d'attaque semblables à ceux du vote en ligne. Elles doivent également faire l'objet de recherches, et non d'essais.

- Comme mesure immédiate à prendre pour examiner le vote en ligne, on pourrait demander à des chercheurs canadiens, munis des protections juridiques appropriées (ayant préséance sur toute réclamation pour violation des droits de propriété intellectuelle), d'inspecter en détail et en public tous les systèmes de vote en ligne actuellement disponibles au Canada.

- Si le gouvernement décide d'aller de l'avant pour concevoir des ordinateurs de vote en ligne et/ou de vote électronique, les travaux de conception doivent se faire sous le regard du public, à l'aide d'une source ouverte, conformément aux principes du gouvernement ouvert. Les principales caractéristiques d'une telle conception ouverte sont les suivantes :

    - permettre en tout temps l'inspection et la mise à l'épreuve de tous les codes de vote par le public;
    - s'assurer que la loi permette à tout enquêteur sur les questions de sécurité (y compris un membre du public) de soumettre les systèmes de vote en ligne et de vote électronique à des épreuves, y compris les systèmes provenant de tiers;
    - si une technologie de tiers (p. ex. provenant de sociétés à but lucratif) est utilisée pour les machines de vote en ligne et de vote électronique, ne pas permettre qu'une inspection de cette technologie ne soit pas menée pour des motifs de protection de la propriété intellectuelle. Il n'y a aucune sécurité par l'obscurité.

- Avant de procéder au déploiement technologique, le gouvernement doit établir le prix détaillé du cycle de vie complet de toute technologie utilisée, y compris les frais d'entretien, de mise à niveau, d'entreposage physique et d'hébergement.

Section 3 : Éléments de preuve à l'appui

Coercition

La ministre Maryam Monsef a été éloquente sur la question de la coercition. À la table ronde sur le vote en ligne tenue le 26 septembre 2016, elle a déclaré : « En outre, comment savons-nous que la personne qui clique […] son vote en ligne n'est pas forcée, peut-être pas un partenaire violent ou coercitif d'une certaine façon? Il peut s'agir d'une personne ayant un problème d'accessibilité ou un handicap qui est persuadée par une autre personne de voter d'une certaine façon. Comment peut-on s'assurer que l'intégrité du vote, que la confidentialité du vote, est préservée? » [TRADUCTION] (Monsef, 2016)

Dans sa présentation TEDx intitulée *Internet Voting? Really?* (Voter par Internet, vraiment?), Andrew Appel raconte l'histoire du vote aux États-Unis, en commençant par la méthode de vote originale, celle de simplement dire son choix à haute voix, en public. Il a clairement expliqué que le scrutin secret et les procédures de confidentialité en place dans les bureaux de vote ont été précisément conçus pour réduire le risque de coercition. (Appel, 2016)

Chaîne de possession

Dans une vidéo de Computerphile, Tom Scott a clairement décrit la question de la chaîne de possession : « Seriez-vous satisfait […] qu'une personne téléphone à une autre personne pour lui dire son vote, et que toutes ces personnes promettent de garder le secret jusqu'à la toute dernière personne appelée, qui a promis de compter tous les votes avec exactitude et qu'à la fin de l'élection, tous ces gens, seuls à la maison, ayant donné leur vote en privé par téléphone se fassent tout simplement annoncer qui a gagné? Parce que c'est en gros ce qu'est le vote électronique. » [TRADUCTION] (Scott, 2014)

Cyberattaques fructueuses contre le gouvernement canadien

Selon les données, deux grands types d'attaques visant les ministères du gouvernement canadien ont été perpétrés avec succès à ce jour. La première, en 2011, a compromis le ministère des Finances, le Secrétariat du Conseil du Trésor et Recherche et développement pour la défense Canada. (Weston, 2011) (Ljunggren, 2011) La seconde, en 2014, a compromis le Conseil national de recherches du Canada. (Barton, 2014) (Secrétariat du Conseil du Trésor du Canada, 2014) (Freeze, 2016)

Questions liées à la sécurité informatique

La littérature portant sur les questions de sécurité informatique ayant trait au vote en ligne et au vote électronique est tellement volumineuse et contient tellement de déclarations de scientifiques informatiques qui ne recommandent pas le vote en ligne qu'il faudrait rédiger un document d'information distinct pour leur rendre justice. Heureusement, Eric Geller a écrit un tel rapport, intitulé *Online voting is a cybersecurity nightmare*. (Geller, 2016) Sous un angle plus universitaire, l'expert en sécurité informatique J. Alex Halderman a consacré le chapitre d'un livre, *Practical Attacks on Real-world E-voting*, à décrire en détail les failles réelles (et non théoriques) des divers systèmes de vote en ligne et de vote électronique.

L'élément le plus notable se trouve dans la section sur le vote par Internet : il y fait rapport de la façon dont le système de Washington, DC a été piraté par des chercheurs externes invités à en éprouver la sécurité avant l'élection, ainsi que des nombreuses failles de sécurité opérationnelle du système de vote par Internet de l'Estonie qu'ont constatées des chercheurs externes invités à l'inspecter. (Halderman, 2016)

Il existe également une déclaration sur le vote par Internet de la US Association of Computing Machinery, la plus grande association américaine de professionnels en science informatique. Cette déclaration se termine ainsi : « Il faut aux systèmes certains moyens pour préserver la capacité de vérifier et de recompter les votes. Pour le moment, les systèmes qui reposent sur le papier offrent la meilleure technologie qui soit pour ce faire. » [TRADUCTION] (US Association of Computing Machinery, n.d.)

Avertissements des experts en sécurité nationale

Neil Jenkins du département américain de la Sécurité intérieure a déclaré : « […] le vote en ligne, surtout le vote en ligne à grande échelle, présente un énorme risque pour le système électoral en menaçant les attentes des électeurs en matière de confidentialité, de responsabilité et de sécurité de leurs votes ou en offrant aux acteurs malveillants une avenue pour manipuler les résultats de scrutin. » [TRADUCTION] (Horwitz, 2016)

Le secrétaire de la Sécurité intérieure des États-Unis, Jeh Johnson, a déclaré : « ces défis [de cybersécurité] ne sont pas à venir – ils sont déjà présents. […] Dans quelques cas, nous avons découvert que des acteurs malveillants ont eu accès aux systèmes de vote des États. » [TRADUCTION] (Johnson, 2016)

Participation électorale, y compris celle des jeunes

Selon le rapport de 2012 de la Ville de Kitchener sur le vote par Internet : « Il est très clair que, peu importe le lieu de résidence, le vote par Internet n'attire pas les jeunes électeurs. » [TRADUCTION] (Gosse, 2012) Dans le même ordre d'idées, le groupe d'experts indépendants sur le vote par Internet de la Colombie-Britannique a déclaré, dans son rapport de 2014, que « la recherche donne à penser que le vote par Internet n'encourage généralement pas les personnes qui ne votent habituellement pas à changer leurs habitudes à ce chapitre. Le vote par Internet est surtout un outil pratique pour les personnes qui ont déjà choisi de voter. » [TRADUCTION] (Archer, Beznosov, Crane, King et Morfitt, 2014)

Exemples de constats sur le vote en ligne provenant d'autres pays

Pour ne citer que trois exemples, disons que le Royaume-Uni et la Norvège ont cessé le vote en ligne après des essais en raison de problèmes de sécurité et autres préoccupations, alors que l'Australie, après une enquête approfondie d'un comité parlementaire, a conclu que le pays n'était « pas en position de mettre en place un système de vote électronique à grande échelle dans un proche avenir sans très lourdement compromettre son intégrité électorale. » [TRADUCTION] (Glover et Branigan, 2005) (BBC News, 2014) (Parlement de l'Australie, Joint Standing Committee on Electoral Matters, 2014)

Ouvrages cités

Appel, A. (26 mars 2016). *Internet Voting? Really?* | *Andrew Appel* | *TEDxPrincetonU [fichier vidéo]*. Tiré de YouTube : https://youtu.be/abQCqIbBBeM

Archer, K., K. Beznosov, L.-A. Crane, V. King et G. Morfitt. (12 février 2014). *Recommendations Report to the Legislative Assembly of British Columbia.* Tiré de l'ouvrage *British Columbia Independent Panel on Internet Voting* : http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

Barton, R. (29 juillet 2014). *Chinese cyberattack hits Canada's National Research Council*. Tiré de CBC News : http://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

BBC News. (27 juin 2014). *E-voting experiments end in Norway amid security fears*. Tiré de BBC News : http://www.bbc.com/news/technology-28055678

Freeze, C. (2 septembre 2016). « Canadian research body relied on paper communications after Chinese hack, documents show ». Tiré du *Globe and Mail* : http://www.theglobeandmail.com/news/national/records-show-extensive-fallout-from-chinese-hack-of-national-research-council/article31695327/

Geller, E. (10 juin 2016). « Online voting is a cybersecurity nightmare ». Tiré de *The Daily Dot* : http://www.dailydot.com/layer8/online-voting-cybersecurity-election-fraud-hacking/

Glover, J. et T. Branigan. (7 septembre 2005). « E-voting plans shelved after extensive trials ». Tiré de *The Guardian* : https://www.theguardian.com/technology/2005/sep/07/egovernment.politics

Gosse, R. (10 décembre 2012). *FCS-12-191 - Alternate Voting – Internet Voting.* Tiré de City of Kitchener - Laserfiche WebLink : http://lf.kitchener.ca/uniquesig0d1d2aa1a38f6e69dc1e79e99d780c34f537a34d9c901a0d7cbb1976cbfdd057/uniquesig0/WeblinkExt/0/doc/1235356/Page1.aspx

Halderman, J. A. (2016). *Practical Attacks on Real-World E-Voting*. Dans F. Hao et P. Y. Ryan (Éd.), *Real-World Electronic Voting: Design, Analysis and Deployment* (pp. 145–171). CRC Press. Tiré de https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf

Horwitz, S. (17 mai 2016). « More than 30 states offer online voting, but experts warn it isn't secure ». Tiré du *Washington Post* : https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/

Johnson, J. (1er octobre 2016). *Statement by Secretary Johnson About Election Systems' Cybersecurity*. Tiré de US Department of Homeland Security: https://www.dhs.gov/news/2016/10/01/statement-secretary-johnson-about-election-systems-cybersecurity

Ljunggren, D. (17 février 2011). *Canada says cyber-attack serious, won't harm budget*. Tiré de Reuters Canada : http://ca.reuters.com/article/topNews/idCATRE71G0RG20110217

Monsef, M. (26 septembre 2016). *Voting Reform : Online Voting Roundtable – Maryam Monsef [fichier vidéo]*. Tiré de CPAC – La Chaîne d'affaires publiques par câble : cpac.ca/en/electoralreform/ – *Electoral Reboot: What you need to know as MPs*

consider how you elect them! : http://www.cpac.ca/en/jwplayer/?params=ZXA9NDkwMjE5NTUmcD1odHRwJTNBJTJGJTJGd3d3LmNwYWMuY2ElMkZ3cC1jb250ZW50JTJGdGhlbWVzJTJGY3BhYyUyRl9yZXNvdXJjZXMlMkZfaW1hZ2VzJTJGc3RydWN0dXJlJTJGQ1BBLTk2MC03MjBfRGlnaXRhbEFyY2hpdmVfZW4uanBlZyZzaGFyZT0=&time=172.054

Parlement d'Australie – Joint Standing Committee on Electoral Matters. (novembre 2014). *Second interim report on the inquiry into the conduct of the 2013 federal election: An assessment of electronic voting options*. Tiré du site Web du Parlement de l'Australie : http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Second_Interim_Report

Scott, T. (18 décembre 2014). *Why Electronic Voting is a BAD Idea – Computerphile [fichier vidéo]*. Tiré de YouTube : https://youtu.be/w3_0x6oaDmI

Secrétariat du Conseil du Trésor du Canada. (29 juillet 2014). *Archivé – Déclaration de la dirigeante principale de l'information du gouvernement du Canada*. Tiré du site Web du gouvernement du Canada : http://nouvelles.gc.ca/web/article-fr.do?nid=871449&_ga=1.209142609.232256221.1470410176

US Association of Computing Machinery. (n.d.). *Internet Voting*. Tiré de ACM US Public Policy Council : http://usacm.acm.org/evoting/category.cfm?cat=30&E-Voting

Weston, G. (16 février 2011). *Foreign hackers attack Canadian government*. Tiré de CBC News : http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618